DOE

C I A C

Computer Incident Advisory Capability

UCRL-AR-118607/CIAC 2304

Data Security Vulnerabilities of Facsimile Machines and Digital Copiers

CIAC-2304

by William J. Orvis and Allan L. Van Lehn

January, 1995

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1/1/1995	Report 1/1/1995

4. TITLE AND SUBTITLE
Data Security Vulnerabilites of Facsimile Machines and Digital Copiers

5. FUNDING NUMBERS

6. AUTHOR(S)
William J. Orvis and Allan L. Van Lehn

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

DOE Computer Incident
Advisory Capability (CIAC)
Lawrence Livermore National
Laboratory

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

This study examines the data security vulnerabilities of facsimile machines, i.e., self-contained fax machines and fax modems. This study is primarily concerned with vulnerabilities associated with outsider intrusion and interception. An outsider is anyone who does not have physical access to the fax machine, but does have access to the phone number, wires, utilities, and trash that passes into and out of the facility containing the fax machine. This paper investigates the possibility of an outsider compromising data without that person ever touching the fax machine.

14. SUBJECT TERMS
IATAC Collection, information security, data security threats, vulnerabilities

15. NUMBER OF PAGES
45

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (615) 576-8401, FTS 626-8401.

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Table of Contents

Table of Contents, Continued

Table of Contents, Continued

Introduction

Overview

This study examines the data security vulnerabilities of facsimile machines, i.e., self-contained fax machines and fax modems. This study is primarily concerned with vulnerabilities associated with outsider intrusion and interception. An outsider is anyone who does not have physical access to the fax machine, but does have access to the phone number, wires, utilities, and trash that passes into and out of the facility containing the fax machine. This paper investigates the possibility of an outsider compromising data without that person ever touching the fax machine.

This study also includes vulnerabilities associated with an insider, but only generally, because of the large number of access avenues available to an insider. An insider is an individual who has physical access to the fax machine, its input and output papers.

This study did not attempt to review all manufactured facsimile machines. Furthermore, we do not claim to have discovered all the vulnerabilities of the machines tested. And machines not tested may have vulnerabilities peculiar to a unique feature or due to a specific weakness in a certain make and model.

This study also examines those smart copy machines whose capabilities parallel fax machines.

What's in this Study

Included in the study is:

- general information about fax machines (description and history of fax machines).
- information about the fax machines tested for this study.
- an explanation of the data security threats.
- an explanation of the vulnerabilities.
- recommendations for decreasing the threats and vulnerabilities.

About Fax Machines

What Is a Fax Machine?

Fax or facsimile machines are devices for transmitting an image of a document over telephone lines. The transmission method is standardized world wide, so that a fax can be sent between nearly any two fax machines made by different manufacturers anywhere in the world (see Appendix A).

History of the Fax Machine

Facsimile is the oldest office automation technology, predating the telephone and telegraph. The first fax machine model was invented by the Scottish inventor Alexander Bain in 1842, using a pendulum to create images on a shellac-coated piece of metal. As you might expect, it didn't work very well, with the major problem being the synchronization of the sending and receiving pendulums. Some manner of improvement was achieved by Ludovic d'Arlincourt, by using tuning forks to synchronize the sending and receiving machines. It wasn't until 1902 that Arthur Korn created the first direct descendent of the modern fax machine by using photocells to scan a photograph and transmit the image over wires. This and later systems were used heavily by newspapers to transmit photos across the country and overseas.

Practical modern fax technology did not flourish until 1980, with the adoption of the Group 3 digital fax standard by the International Telecommunications Union (ITU, see Appendix B). This standard made possible the interoperation of fax machines from different vendors. Since everyone with a fax machine that followed the standard could share documents, the use of fax grew rapidly.

Today, facsimile handles more messages than any other electrical communications system except voice. As of 1992, more than nine million facsimile units were in use.

How a Fax Machine Works

A modern Group 3 fax machine sends a document by scanning it and converting that scan into telephone compatible tones. To receive a document, a fax receives the tones from the telephone and converts them back into a digital image. That image is then printed. Figure 1 is a diagram of a typical fax machine.

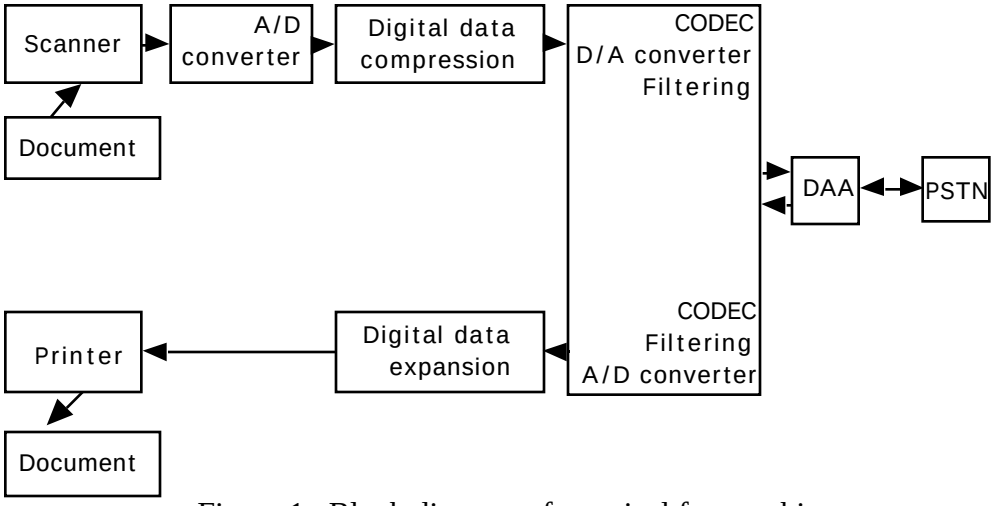


Figure 1. Block diagram of a typical fax machine.

An outgoing fax follows the upper branch in the figure. A document is placed in the scanner and scanned. The scanned image is converted into a digital image using an analog to digital (A/D) converter. The digital image is passed into the digital data compression and coding unit that converts the image into standard fax coding. The next sections consists of the coder/decoder (CODEC) and the data access arrangement (DAA). These two blocks together form a standard digital modem, the same as is used with general purpose computers to communicate with remote computers via telephone lines. The compressed digital image passes to the CODEC where it is converted into an analog signal that is compatible with the telephone network and filtered to reduce noise. This analog signal passes into the DAA, which serves as the interface between the fax machine's electronics and the public service telephone network (PSTN). The DAA is an analog device that handles connections to remote systems and isolates the PSTN from the fax machine.

An incoming fax flows backward along the bottom branch in the figure. The analog signal comes in from the PSTN into the DAA and into the CODEC where it is filtered and converted back into a digital signal. The digital signal passes into the data expansion unit where compression is reversed and then converted back into an image. The image is typically sent to a printer for printing.

Older Table-top Fax Machines

Old machines (Group 1, Group 2) are primarily analog machines with little in the way of electronic intelligence. They operate much the same way as the Group 3 fax machine shown in figure 1 except they do not convert the image into a digital signal. The analog signal from the scanner is passed directly to the DAA where it is placed on the telephone lines. These machines have no data compression or correction capability which causes slower operation and poorer image quality. Appendix B has additional information about Group 1 and Group 2 fax machines.

New Table-top Fax Machines

Modern fax machines began with the adoption of the Group 3 digital standard in 1980. Generally, they are fully digital devices that use new modem and data compression technologies to speed fax transmissions. The Group 3 standard was written to anticipate the introduction of higher speed modems to produce higher speed fax machines as the technology improves. Appendix B has additional information about Group 3 fax machines.

About Fax Modems

Fax Modems

The fax modem shown in Figure 2 is a relatively new technology that was not usable before the digital fax standard was available and desktop PCs came into widespread use. Fax modems attach to a computer the same way as a standard modem does. In fact, most newer modems combine the capability of a fax machine and a modem into the same chip set. Communication between the computer and the fax modem uses a high-level command set that is much like the Hayes[1] command set used to communicate with compatible modems. By sending the appropriate commands, a computer can command a fax modem to dial and connect to a fax machine and send or receive a fax. Only the fax data is captured by the modem. Special software is needed to turn the encoded fax image into an image that can be seen on the screen or printed.

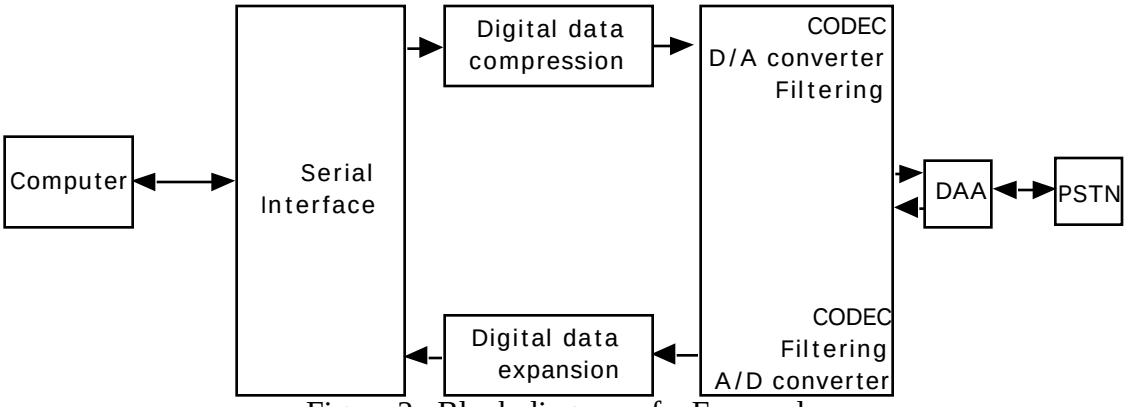


Figure 2. Block diagram of a Fax modem

Fax Modem Chipsets

AT&T, Rockwell, Exar and Sierra have standard, fax modem chipsets available, complete with wiring diagrams on how to use them to create a fax modem. Manufacturers have created a multitude of fax modems based on one of these chipsets. The chipsets are inexpensive and sufficiently easy to use so that a home-made fax modem can be built by an electronics hobbyist. (Ref. 2). This ease-of-use also makes it possible to create an inexpensive fax interception device. Previously, fax interception devices cost many thousands of dollars. This development brings this capability into the realm of the electronics hobbyist.

Fortunately, an inexpensive fax modem cannot be changed into an interception device by simply changing some of the connections. To do so requires reprogramming the onboard computer.

[1] Hayes Microcomputer Products, Inc. developed a modem protocol that has become a *de facto* modem standard.

About Fax Printers

Overview	The type of printer can make a big difference in the security of a fax machine. A description of various print processes follows.
Xerographic Printers	Xerographic printers draw the image on a light sensitive drum. Powdered ink is attracted to the charged drawing on the drum and then rolled onto a piece of paper. The ink is fused to the paper with a hot roller. This is the standard mechanism used in modern copy machines.
Thermal Transfer Printers	Thermal transfer printing transfers ink from a plastic film to the page. A hot print head heats the ink on the film, causing it to stick on the paper. Thermal transfer printers can print on plain paper and are relatively inexpensive compared to xerographic process printers.
Thermal Paper Printers	Thermal paper printers print on heat sensitive papers. A hot printhead pointer causes the paper under it to change color. These are very inexpensive printers, but they require special paper.
Jet Ink Printers	Jet ink printers use liquid ink that is sprayed onto the paper to produce the image.

The Fax Machines Tested in this Study

Overview

The following three fax machines were selected for testing. Each make and model has a common set of operations and vulnerabilities. However, most have unique functions or features that may introduce additional problems.

- Xerox 7033
- Cannon Fax-730
- SpectraCom P1414MX fax modem

Xerox 7033

The Xerox 7033 is a top-of-the-line fax machine that uses a thermal transfer process to print on plain paper. It has memory that can be used to store fax documents in incoming mailboxes to support delayed printing or polling, and for delayed sending. Polling and mailboxes are selected using touch tone signals from the calling telephone, thus polling can be done with any kind of fax because the signaling does not depend on the fax machine but on the telephone.

Cannon FAX-730

The Cannon FAX-730 is an older model fax machine that uses a thermal printing process. It has memory that can be used for mailboxes, polling, and delayed sending. The machine uses a proprietary protocol for polling and mailboxes and thus can only do polling and mailboxes with another machine that uses the same protocols.

SpectraCom

The SpectraCom P1414MX fax modem is a portable, external fax modem that works with any serial communication device. It is attached to a Macintosh running the FAXstf software. It uses the AT&T chipset and can send and receive data or fax at 14.4K baud. It has no polling or mailbox capability. Incoming and outgoing fax documents are stored on an attached computer.

Threats to Fax Machines

Overview

The threats listed in this section are primarily limited to situations where the intruder has access to the communication channel, from the originating fax machine through the public switched telephone network (PSTN) to the receiving fax machine, as shown in Figure 3.

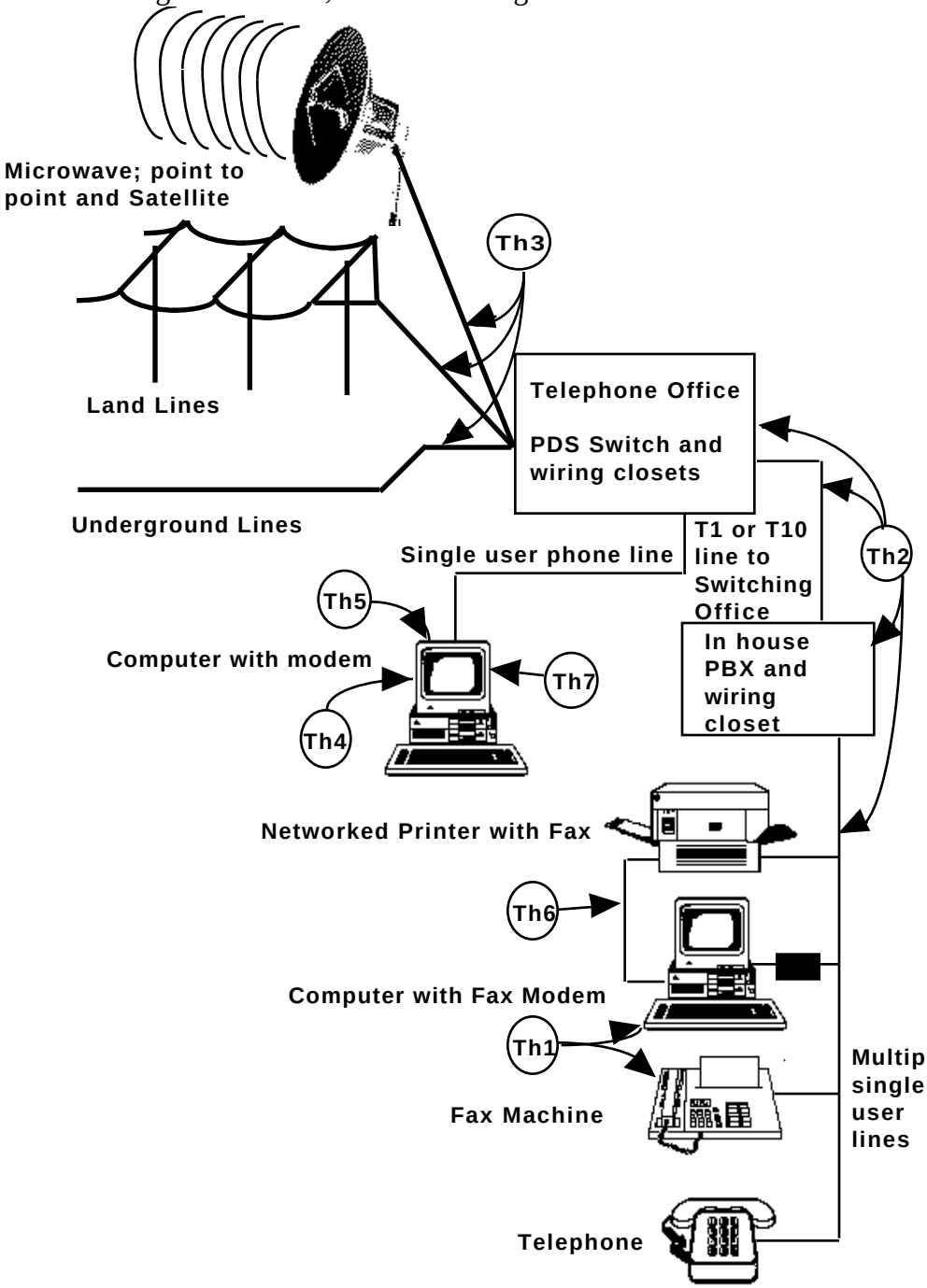


Figure 3. Possible threats to a fax transmission along a public switched telephone network. Threat numbers in circles relate to threat categories in the following text.

Threats to Fax Machines, Continued

Th1 - Physical Access to the Machine	Anyone who has access to a fax machine is a potential threat. This includes human error by a regular user or someone from another area, unfamiliar with the machine; service personnel; or an insider who is also an intruder or interceptor.
Th2 - Physical Access to the Phone Line	Anyone who has access to the phone line that attaches to the fax at any point before it reaches the PDS Switch is a potential threat. This point of access may be along the wire from the fax to the patch panel or in-house PBX, at the patch panel or PBX, along the trunk to the phone company's switching center, or in the switching center.
Th3 - Physical Access to the Trunk Line	Also a potential threat, is anyone who has access to the T1 or T10 trunk line beyond the PDS switch. This includes access to microwave signals using an interception antenna. Phone/Fax intercept devices are available to select any one of the 24 channels in a T1 line and capture a fax being sent on that line. Sophisticated Fax intercept equipment can be expensive, in the $10K to $25K range.
Th4 - Electronic Access to the PDS Switch	Anyone with remote, electronic access (e.g. a phone phreak) to the PDS switch, and the knowledge of how to reprogram the switch can be a threat. The switch controls what physical telephone line a particular phone number is attached to, so control of this switch allows an intruder to divert or party line any local phone number.
Th5 - Electronic Access to the Phone Number	Anyone with the phone number of the fax machine can be a threat.
Th6 - Electronic Access to the Computer Network	Anyone who has access to a networked fax modem or a networked printer with an internal fax modem is potentially a threat. This access is on the input side of the fax modem, including any file servers used to spool fax messages.
Th7 - Computer-controlled Fax Modems	Anyone who uses computer-controlled fax modems to automatically dial phone numbers to search for fax machines and transfer the station message is a threat.

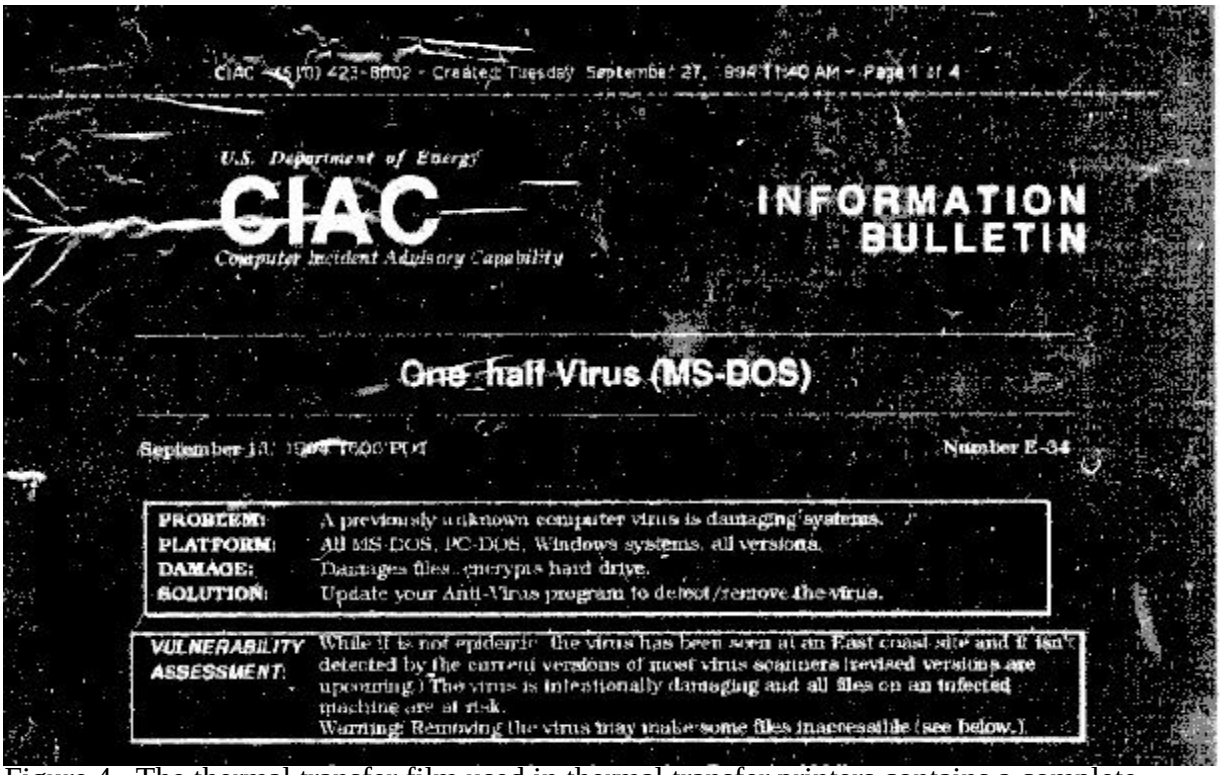
Vulnerable Characteristics of Fax Machines

Overview	Complementing the threats are characteristics of fax machines that provide avenues for intrusion. This section lists those characteristics of fax machines that lead to vulnerabilities.
C1 - No Authentication of Fax Messages	There is no standard authentication method for verifying fax messages. Authentication, if done at all, is on a manufacturer-by-manufacturer basis. The only standard identifications are the station message, the provider ID, and the subscriber ID.
Station message	The station message is entirely arbitrary and can be set by anyone with physical access to a machine.
Subscriber ID	The subscriber ID is supposed to contain the phone number the machine is attached to, but can be set to anything by anyone with physical access to the machine.
Provider ID	The provider ID identifies the manufacturer of a machine and lists non-standard features, enabling interaction with other machines from the same manufacturer. The provider ID is not changeable by a normal user, but could probably be changed by a determined intruder with the capability to produce a new ROM for the machine. ROM programming equipment that attaches to a personal computer can be obtained by anyone for under $200.
C2 - No Authentication of Features	No standard authentication method has been designed for polling, store and forward, and the mailbox features of fax machines. Since FAX has traditionally been a point-to-point messaging system, the phone number is the only authentication used, and phone numbers can be spoofed.
C3 - No Message Encryption	Fax messages are not normally encrypted; therefore any listening device can reconstruct the message. Encryption is available as an add-on capability, but machines with encryption can only be used with a machine that has a complementary decryption capability.
C4 - Difficult and Confusing Setups	Setting up a fax with all its options is often difficult and confusing. The manuals that come with the faxes are usually filled with procedures to follow, but they do not always give an explanation as to why you would want to follow them. Some manuals appear to be crude translations of manuals written in another language. The result is often incorrect set up or machines left in their default, and often vulnerable, configuration.

Vulnerable Characteristics of Fax Machines, Continued

C5 - No Safeguards for the Untrained or Careless User	There are no safeguards for the untrained or careless user. If a user does something that could be wrong (e.g., making polling open to any machine that calls), the fax machine does not warn them in any way. Some machines do have an operator password feature to prevent others from reprogramming the machine, but the operator often has the same training as the causal user (none) and so is just as likely to make mistakes in the set up.
C6 - Hardware Limitations	Hardware is often limited in its ability to do some things such as sanitizing a machine to eliminate a document from memory.
C7 - No Delivery Information	Facsimile is a station-to-station messaging system; i.e., the sending machine is directly connected to the receiving machine. Thus, no delivery information is included in the standard. Since most fax machines are shared by multiple users, a cover sheet with the recipients names has become a standard mode of operation to let the receiver know who is to receive the fax. This situation is apt to change very soon for networked fax modems so that incoming messages can be routed electronically to the correct recipient without a human having to read a cover sheet and route manually.
C8 - Thermal Transfer Printers	Thermal transfer printers leave a negative image of the printed page on the thermal transfer film. If the film is not carefully disposed of, it can give an intruder a complete copy of all faxes printed on a machine (see Figure 4).

Vulnerable Characteristics of Fax Machines, Continued


CIAC (510) 423-8002 - Created: Tuesday September 27, 1994 11:40 AM - Page 1 of 4

U.S. Department of Energy

CIAC

Computer Incident Advisory Capability

INFORMATION BULLETIN

One_half Virus (MS-DOS)

September [illegible] Number E-34

PROBLEM:	A previously unknown computer virus is damaging systems.
PLATFORM:	All MS-DOS, PC-DOS, Windows systems, all versions.
DAMAGE:	Damages files, encrypts hard drive.
SOLUTION:	Update your Anti-Virus program to detect/remove the virus.

VULNERABILITY ASSESSMENT: While it is not epidemic, the virus has been seen at an East coast site and it isn't detected by the current versions of most virus scanners (revised versions are upcoming.) The virus is intentionally damaging and all files on an infected machine are at risk.
Warning: Removing the virus may make some files inaccessible (see below.)

Figure 4. The thermal transfer film used in thermal transfer printers contains a complete readable record of every item printed and is susceptible to intercept if it is not protected and properly destroyed.

Vulnerabilities and Unintentional Exploitation

Overview

This section describes the problems arising from accidental or unintentional causes. Each vulnerability is mapped to the threat(s) (represented by the Th#) and characteristic(s) of the fax machine (represented by the C#) that cause or allow the vulnerability.

Wrong Telephone Number - Th1, C4, C5

One of the most common mistakes made when sending a fax is dialing the wrong telephone number. For hand-dialed systems, a misdial usually results in hitting a voice number, so nothing is compromised. On the other hand, in speed dialing situations, typing the wrong speed dial button sends the fax to a real fax machine; it's just the wrong one. Some speed dial numbers can be set to send to 50 or more different fax numbers with the press of a single button. An unconfirmed report tells of an internal briefing document being sent to 50 state governors when a staff member pressed the wrong speed dial button.

Wrong Printer Driver - Th1, C4, C5

Fax modems attached to personal computers usually behave like printers. The existing print capabilities of the personal computer are used to format the document. The formatted document is then sent to the fax modem instead of to a printer. If the user sends a fax and then forgets to reset the printer driver to the normal printer, the next document printed is sent to the fax instead of to the printer. Luckily, the additional set up needs of a fax, such as selecting the phone number to send to, usually makes this error obvious . The user can abort the process before the document is actually transmitted.

Problems with Setting Up the Polling Feature - Th5, C5

Polling is one fax calling another fax to request that it send any waiting fax messages. In most situations, the machine being polled checks the station message of the calling machine and only sends the message to it if it is an authorized machine. If the setup is done incorrectly, the machine being polled sends any stored fax messages to whomever calls first. If an intruder knows that a machine is not configured correctly, he can continuously call the machine and obtain any waiting fax messages.

Set up of polling is not standard and most users do not even know of this capability. They might activate it while experimenting with the settings, opening the polling door to whomever requests it.

Mailboxes without Passwords - Th5, C5

Mailboxes are similar to polling but faxes are stored for specific individuals or machines. Leaving out a mailbox password allows an outsider to access any faxes stored in that mailbox. It also makes it possible for a fax machine to be used as a “drop box” for others to store information for their associates. Such use, if discovered could range from an embarrassment to much worse if illegal operations are involved. The unsavory are attracted by the ease of and low risks associated with making illegal deals by fax. Mailboxes have the same setup problems as polling.

Incomplete Sanitizing - Th1, C4, C6

Sanitizing a machine after sending a sensitive unclassified or classified fax, presumably using an encrypting phone set such as a STU phone, by pulling the plug may not work on some of the newer fax machines. Fax messages are typically buffered in memory but may be on an internal disk drive or the memory may be nonvolatile FLASH RAM or may be backed up by battery. Fax machines with internal hard drives have the capability of holding thousands of fax images. Even though the data is "deleted" after the fax is sent, the data still exists on the disk drive which could be removed and the data retrieved.

> ☞ **Note: It is essential to determine and execute complete sanitization steps for any fax machine handling sensitive unclassified or classified data before switching its STU phone back to normal transmission.**

Print Mechanism Problems - Th1, C5

Print mechanism problems could also come under the heading of incomplete sanitizing. Print mechanism problems occur when the printing method leaves remnants of the previously printed document in a readable state. Fax machines that use thermal print heads and special paper are generally not a problem. However, thermal transfer printers that use an ink coated plastic film generally leave a negative image of the printed document on the film. If the film is thrown in the trash, anyone finding the used film has a complete record of every fax received and printed by the machine.

Plain paper printers that use the xerographic process are less of a problem than thermal transfer printers. Xerographic process printers have the same vulnerabilities as copy machines, that of image retention on the image transfer drum. Retrieving the image from the image transfer drum is not a simple process, and printing a few blank pages after printing a sensitive document will usually obscure any retained image.

Printer Paper Problems - Th1, C5

Printer paper problems could also be described as junk mail or denial of service problems. The paper supply is finite for each loading. The number of incoming faxes can easily surpass the amount of paper during times of unattended operation. Occasionally, incompatible fax transmissions can cause a whole roll of paper to be spewed out with little or no valid information printed. A deliberate repeated sending of junk faxes could be done to deny normal fax service.

Distribution Problems - Th1, C1, C2, C3

Fax messages appearing in a machine's output tray can be read by anyone searching for a personal fax because there is no authentication of, or privacy in routing to, the receiving individual. Intruders with access to the fax machine could read every message that appears in the output tray.

Vulnerabilities Exploitable by Intruders

Overview

This section describes the vulnerabilities that may be actively exploited by intruders. Each vulnerability is mapped to the threat(s) (represented by the Th#) and characteristic(s) of the fax machine (represented by the C#) that lead to the vulnerability.

Relay Broadcasting - Th5, C1, C3

Most modern fax machines have a "store and forward to multiple locations" capability. The forwarded fax documents may go to several different machines. This capability is used to save long distance charges by sending a single fax long distance to a relay broadcasting machine that then sends it to multiple local numbers. Forwarding machines may immediately send the fax or may hold it until they are polled by the recipients.

In polled situations, if the intruder knows the number of a machine that does polling, (s)he can call and get its system message. By programming that system message into their machine and calling the machine that contains the faxes waiting to be forwarded, they intercept the fax. After receiving the fax and making a copy, the intruder can cover his or her tracks by changing their station message to that of the polled system and resending the fax to the original polling system.

Another way to intercept a broadcasting system is to call the manager of the forwarding machine and fool the manager into thinking that they are a normal recipient. By asking the manager to use a "new number" they get their machine to be a recipient. This is one example of what it commonly called “social engineering.”

An intruder with physical access to a broadcast machine could bypass the social engineering and directly add his/her own number to the list of numbers and thereafter receive a copy of all broadcast faxes.

Mailboxes without Passwords - Th5, C2, C4

The use of mailboxes on fax machines has not been standardized. In order to be compatible with machines made by other manufacturers, the Xerox 7033 fax machine uses touch tone signals to select a mailbox before fax transmission begins. A user calls in, types the mailbox number on his telephone and starts a manual receive operation on his fax. The Xerox then sends the contents of the selected mailbox. There is no security on the mailbox, so a person could simply go down the list of mailboxes and get the contents of each. A 4-digit mailbox number has only 10,000 possibilities which could easily be tried in a short time by a computer-controlled fax modem.

Polling - Th5, C2, C5

Polling problems are just as vulnerable to an intruder as mailboxes. If the polled machine does *not* require a password, then any machine could call up and obtain a waiting fax.

Vulnerabilities Exploitable by Intruders, Continued

Local Rerouting - Th1, C1, C3	Depending on the access or skills of an intruder, phone lines or calls can be rerouted to another machine so that machine receives the fax. The only indication of this problem would be if you received a phone call from the sender seeking confirmation that you received the fax before the intruder could resend it to you. With insider access, almost anything can be done. An intruder's fax machine could be put under the table or down the hall from a target machine and telephone wire strung between them. All incoming faxes would be stored and printed on the intruder's machine, which would then send them on to the target machine. By changing the phone number and station message of the intruder's fax to match those on the received fax, the target fax could be fooled to think that no interception had occurred.
Phone Taps - Th2, C1, C3	With access to the phone lines, an intruder can tap the phone line and intercept the fax traffic. Tapping the line is usually easy for the intruder, because phone patch panels are generally in secluded areas, such as closets or basements. Thus, the intrusion is unlikely to be noticed. Detecting phone taps is a matter for specialists using sophisticated electronics.
Phone Company Rerouting - Th4 , C1, C3	Phone phreaks, people who perform illegal operations to cheat or defraud phone companies and their regular customers, can reroute phone numbers by taking control of the PDS switches at the phone company. Phone phreaks are known for being able to reroute phone numbers and create party lines. Using this capability, an intruder can reroute fax phone numbers to their fax machines, print the faxes, then send them to the target machines. This kind of interception is very difficult to detect.

Vulnerabilities Exploitable by Interceptors

Overview

This section describes the vulnerabilities exploitable by interceptors. Each vulnerability is mapped to the threat(s) (represented by the Th#) and characteristic(s) of the fax machine (represented by the C#) that can cause the vulnerability.

Intercepting Dialouts - Th1, Th2, Th3, Th4, Th5

With physical access to the machine, phone line, trunk line or electronic access to the PDS switch, an interceptor can reroute phone numbers by taking control of PDS switches at the phone company. Interceptors can reroute fax phone numbers to their fax machines, print the faxes, then resend them to the target machines. With electronic access to the phone number, the interceptor opens a connection to a machine after it checks for dial tone, but before it has made a connection. The result is that the fax machine thinks it is talking to one number, when in fact, it is talking to another. This method of attack has been used successfully to break into bulletin board systems (BBSs) and is applicable to fax machines because they use the same modem technology.

Commercial Interception Hardware - Th1, Th2, Th3, C3

Commercially developed telephone and facsimile interception devices are sold to security and law enforcement personnel, and are most likely available to people involved in industrial espionage. Devices are available that can tap a T1 trunk line and extract any one of the 24 multiplexed phone conversations. If the conversation is a fax transfer, the machine can copy and display it. The cost is significant, in excess of $10K for a machine that can connect to a T1 trunk line. Such devices are very hard, if not impossible to detect.

Home-built Interception Hardware - Th1, Th2, C3

AT&T, Rockwell, Exar and Sierra have created sets of commercial fax chips that comprise nearly complete fax machines. An analog front end and a micro controller are all that are needed to complete a design. AT&T sends anyone who asks a guide on how to create a fax modem using their chips, complete with wiring diagram (Ref. 4). Using these chips, or a modem made with these chips, an inexpensive home fax intercept device could be built. This intercept device would attach to a single line to listen to and record fax traffic.

In an inexpensive fax modem, the fax chips are normally combined with a micro controller to translate between the ASCII commands from the host computer and set the registers that control the chips. Since fax is point-to-point, the existing chips control half of the communication channel and respond to the other half. The chips expect to answer any incoming requests and expect answers when they send a request. This mode of operation would have to be disabled to create an intercept device which has a passive listening mode. By replacing or disabling the micro controller and setting registers externally, one should be able to create an inexpensive intercept device that would work on individual telephone lines. Due to the complexity involved in separating the multiplexed signals on a T1 phone line, it is not likely that an inexpensive intercept device could be made with the chips available today.

Vulnerabilities Exploitable by Interceptors, Continued

Altered Information - Th5, C1	Because the fax number and the station message are arbitrary, it is possible for any machine to send a fax so it appears to have come from some other machine. Using this capability, falsified fax messages could be sent to a machine, fooling it and the recipient into believing that they have received a legitimate fax and that the content of the fax is true.
Party-line Listening for User Names and Passwords - Th4, C3	Phone phreaks are known to have created party lines through access to the PDS switch. If a party line is created between the intruder's phone and a fax line, the intruder can listen to all the fax messages that are passing through that line. With a suitable fax machine to print the sent documents, all fax traffic on that line could be observed, undetected.
Electro-magnetic Radiation - Th4, C3	Unless a facsimile machine is TEMPEST approved, all fax traffic on that machine could be observed, undetected, by sensitive electromagnetic listening devices. TEMPEST approved equipment may be required, depending on applicable government agency policy, for all unshielded computer and communications equipment that is handling classified data (Ref. 8). The DOE requires a TEMPEST threat assessment be performed by each site’s TEMPEST Coordinator. If the threat assessment indicates the need for countermeasures, the TEMPEST Technical Authority at DOE headquarters must give approval for the costs involved (Ref. 9-13).

Recommendations for Purchasing a Fax

Overview

If you are planning to purchase a fax machine, you should consider the problems outlined in this report. The solutions you adopt depend on the amount of security you need.

Print Mechanism

If you are concerned about someone digging through your trash and reading faxes sent to you, establish a procedure for complete destruction of discarded faxes and avoid thermal transfer printers or destroy thermal transfer film. Consider machines that use thermal paper, the xerographic process or some other process that does not leave an image of the fax on a disposable film.

Mailboxes and Polling

If you need mailboxes, you should consider getting a machine with a proprietary mailbox system that requires a mailbox number and a password. A drawback is that you must use compatible systems at both ends. This probably means acquiring the same brand of machine if not the same model in all of your installations.

Because mailboxes and polling are not in the fax standard, there is a trade off here between compatibility and security. To be compatible with a wide number of machines, you must institute a method like that used on the Xerox 7033 fax machine. Using a touch tone phone, any fax machine can connect to the Xerox and receive stored faxes. Unfortunately, this method offers little security to prevent the wrong person from getting the fax. On the other hand, the Cannon fax uses a proprietary mailbox and polling scheme that requires user numbers and passwords to access polled faxes and mailboxes. This is a much more secure system, but has the drawback of being only compatible with similar Cannon fax machines. It may not even be compatible with newer models of the Cannon fax.

Encryption

If security of the sent and received messages is important, the only solution is to use encryption. Either buy a machine that has built-in encryption or use an encrypting modem such as a STU-III. A drawback is that you must use the same encrypting mechanism at both ends of the channel, raising compatibility issues again. The U.S. Government has established DES encryption as the standard for encrypting unclassified information.

> ☞ **Note: A useful addition to the fax standard would be encryption for the information, for station authentication and for digital signatures which are unique for each user. Standardized encryption would make possible secure exchange of data by fax with any other fax machine, world-wide.**

Recommendations for Purchasing a Fax, Continued

Verification

Currently, there is no automatic method for verification of transmitted faxes. You must call the receiver and verify identity over the phone as the fax is sent. This prevents most divert-and-resend scenarios except for the most technical of attackers who have a system that captures and resends a fax simultaneously. A drawback is that there must be someone attending both ends of the fax channel.

For states where it is allowed, caller ID or number ID is a useful option because the phone company is sending you the number, not the calling fax. But even there, a phone phreak presumably can make the phone system send the wrong number to the caller ID display.

Recommendations for Operating a Fax

Overview

How a fax is operated and maintained has a lot to do with the security of the data transmitted by it. Before implementing any severe restrictions on the fax, consider the sensitivity of the information that it will contain. Machines that handle sensitive information demand a different level of security than those that handle public information. Sensitive information might be personal, personnel information or proprietary business information. Public information might be catalog pages and advertisements.

Access

Access is one of the main problem areas. A machine, typically located in a public area to make it easy for employee use, is also easy to compromise. Incoming faxes lay out in the open allowing reading, copying, or theft. Inexperienced users may inadvertently or carelessly perform a compromising operation. Note that facsimile communications can be compromised at either end by a person who has been co-opted; for example, an employee who is being blackmailed or is sympathetic with a cause espoused by an adversarial group. Any fax handling sensitive information should have its access restricted to users who need to know.

When sensitive documents are being sent, the sender and receiver should be in contact during the transmission to insure that the fax has come through and is not being diverted to an inappropriate user. Note that this will not insure that the fax is not being intercepted, just that it is not being diverted.

Maintenance

Maintenance is a problem area if the fax machine uses a thermal transfer printer. Be sure to dispose of the thermal transfer ribbon in such a way that it can not be obtained by an intruder or, inadvertently, by someone going through the trash. Maintenance is also a place where an insider can get access to the internals of a fax machine. Since a maintenance person is supposed to open up a machine and change the electronics, it will not be obvious if that maintenance person is doing something extra such as inserting capture-and-storage electronics that could be removed at the next maintenance interval along with copies of all faxes sent through the machine. The more powerful fax machines can be reprogrammed to save all sent and received faxes, then in the middle of the night resend them, unlogged, to the intruders machine. There are many possibilities for diversion when an intruder has direct access to a machine as powerful as some of the modern fax machines or digital copiers.

Recommendations for Operating a Fax, Continued

Programmable Keys	Programmable keys are a time saver when sending fax documents, automating repetitive operations such as entering commonly used telephone numbers. However, it is very easy to accidentally hit the wrong key and send a fax to the wrong destination. It is also possible for another user or an intruder to reprogram one or more keys. If you use programmable keys, be sure to check the numbers it will dial before using it. Check the station message during the initial connect to ensure you are sending to the correct place. Note also that when dialing instead of using a programmable key, any errors in entering the phone number is likely to connect you to a regular phone, resulting in an aborted call instead of a misdirected fax.
Fax Cover Sheet	Use a fax cover sheet to help ensure that the fax reaches the intended recipient. While this is not a guarantee, a fax without a cover sheet sent to a shared fax machine is very likely to be read by one or more people while attempting to determine whom it is for. Make sure the count of the number of pages being sent (including the cover sheet) is displayed on the cover sheet.
Independent Verification	Official letterhead, message content, signature, and station identification can all be bogus. Prisoners have been released from jail because of falsified orders. Requests for information could come from someone other than the claimant. A policy should be established that independent confirmation is done via another communication channel.
Transmission Report	Check the transmission report to insure that the correct number of pages were sent. On the receiving end, check the number of pages sent on the cover sheet with the actual number of pages to insure that some pages have not gotten mixed up with someone else's fax.
Usage Report	Check the usage report on a regular basis and watch for faxes sent to unknown or inappropriate phone numbers. Especially after sending a fax to a large group of people, check the report to insure that it was sent to your addressee. Check the incoming reports to see that the phone numbers you are receiving faxes from are known and appropriate. You might be able to identify or stop a diversion by detecting an unknown number in the usage report.
Sanitization	If a fax machine is used to send sensitive information, then adequate sanitization procedures are needed to insure that a sensitive image is cleared from memory, from the drum of a xerographic printer or from the ribbon of a thermal transfer printer. Methods of clearing memory are dependent on the particular brand of printer. The drum is cleared by printing some non-sensitive or blank sheets. The ribbon is cleared by cutting out and destroying the piece of ribbon that contains the sensitive data.

Vulnerabilities of Smart Copy Machines

Overview

As an adjunct to this fax machine study, CIAC has considered the new "smart" copiers which use digital electronic methods. Most copiers simply copy from one piece of paper to another and never store the image in the machine. Thus, they are not able to save an image and pass it to someone else. Some persistence still exists on the print drum, but running the next copy or a few blank sheets through it generally removes most traces. Most black and white copiers use this xerographic process so image retention is not a problem. Many color copiers use the thermal transfer process which is a problem. If this is the method used, all your old documents reside on the transfer film that is often thrown in the trash.

Copier Types

There are three types of copiers: analog, hybrid and digital. The distinction is based on how the image is handled between the scanning and printing process. Of the three, the digital or "smart" copiers are the most vulnerable to diversion and alteration.

Analog

The traditional copiers are of this type. The image is scanned optically and the optical image is transferred to a photosensitive drum using mirrors and lenses. The drum then prints the image on a new piece of paper. The only risk here is of persistence of the images on the drum and covert insertion of a digital converter and a means of transmission or storage.

Hybrid

Hybrid copiers use an analog image production method with a computer for handling the interface, troubleshooting, billing, etc. The risks here are the same as for analog copiers except that it might be easier to covertly add a digital interface to a machine that is already digital.

Digital

Digital copiers use a scanner, digital storage, and digital image reconstruction to make copies. Essentially, a digital copier is a scanner, a computer, and a printer in a single box. The scanner scans the image into digital form and passes it to the computer. The computer stores the image in RAM or on disk and can apply image corrections, adjustments, or enhancements. The image may be edited or combined with previously stored images. This makes it possible to paste in pictures, simulate letterhead on each page, or customize each fax sent with names and related information as in a mail-merge operation. The composite image is then printed. These systems are also often capable of fax transmissions and being used as a networked printer for other computers.

Vulnerabilities of Smart Copy Machines, Continued

Potential problems with digital copiers arise because the image is stored on disk where it can be retrieved for viewing by someone else. Pressing the wrong button could transmit the image instead of copying it. The computer program could be modified to store *all* images for later downloading over an attached computer network, or they could be simultaneously transmitted to the adversary's fax machine for printing.

Very often these machines have remote diagnostics connections so that hardware and operational problems can be analyzed by a remote technician via telephone. Remote page counts may be obtained for billing purposes. This service connection is also a potential avenue for an intruder to use to obtain copies of stored faxes.

Translating Copier

The Ricoh Imagio MF530 is a digital copier that translates documents from English to Japanese. The computer contains optical character recognition (OCR) software that converts the English text to Japanese characters which are then printed. This copier also operates as a fax machine and a computer printer. The potential risks associated with this machine are considerable, especially from an insider. This machine not only performs optical character recognition, it must also be able to recognize words and phrases to be able to convert them to Japanese. To do this, it must have a considerable amount of computational power that could be diverted to intrusion activities. For example, the computer could watch for trigger words or phrases and store those documents that contain those phrases for the intruder. Another possibility is that it could be programmed to give an incorrect translation such as adding rude phrases whenever a particular name is mentioned. It could also be able to change the contents of a document during a copy operation.

References

1. Kenneth McDonnell, Dennis Bodson, Richard Schaphorst, *FAX; Facsimile Technology and Applications Handbook*, Artech House, Boston, (1992)
2. Michael Swartzendruber, *High-Speed Modem Basics, Standards and Theory*, Circuit Cellar Ink, June 1993, pp. 38-49
3. Michael Swartzendruber, *High-Speed Modem Basics, The Working Hardware*, Circuit Cellar Ink, July 1993, pp. 38-45
4. AT&T, *Modem Designer's Guide*, Document Number MN92-026DMOS, Oct. 25, 1993
5. AT & T, *AT&T High Speed Modem Data Pump Chip Sets Data Book*, Document Number MN92-058DMOS, June 7, 1993
6. ITU [CCITT] Blue Book, Vol. VII - Fascicle VII.3, *Terminal Equipment and Protocols for Telematic Services, Recommendations T.0 - T.63*, Nov. 14, 1988
7. F. R. McCloud, FAXPIONAGE - WHO'S GOT THE FAX?, S&S News and Views, Vol. 1994, No. 1, pp 7-11
8. J. Wenek, "Facsimilie Security," *Proceedings of NETSEC94*, June 13-15, 1994, Computer Security Institute, (1994)
9. DOE 5639.6A, Classified Automated Information System Security Program, July 15, 1994.
10. DOE M 5639.6A-1, Manual of Security Requirements for the Classified Automated Information System Security Program, July 15, 1994.
11. DOE 5300.2D, Telecommunications: Emission Security (TEMPEST), August 30, 1993.
12. DOE Information Technology Systems Emissions Control Manual, Part 1, June 1994.
13. DOE Technical INFOSEC Criteria for IT Systems Emissions Control, Part 2, February 1994.

Appendix A: Facsimile Machine Standards

What's in this Appendix

This appendix lists the standards documents that apply to fax machines.

Who Sets the Standards

Standards for fax transmissions are primarily set by the International Telecommunications Union (ITU, formerly named CCITT, Consultative Committee on International Telegraph and Telephone), with input from United States standards organizations such as the Electronic Industries Association and the Telecommunication Industries Association (EIA/TIA).

Standards Recommend-ations

The relevant standards recommendations under which most fax machines are manufactured are listed in the tables below.

ITU Facsimile Standard Recommendations

Recommendation	Title
T.2	Standardization of Group 1 Facsimile Apparatus for Document Transmission
T.3	Standardization of Group 2 Facsimile Apparatus for Document Transmission
T.4	Standardization of Group 3 Facsimile Apparatus for Document Transmission
T.4 annex C	File Transfer Using Group 3 Fax Protocols
T.30	Procedures for Document Facsimile Transmission in the General Switched Telephone Network
T.50	International Reference Alphabet
T.51	Coded Character Sets for Telematic Services
T.52	Non-Latin Character Sets for Telematic Services
T.6	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus
T.60	Terminal Equipment for Use in the Telex Service
T.61	Character Repertoire and Coded Character Sets for International Telex Service
T.62	Control Procedures for the Telex and Group 4 Facsimile Service
T.62bis	Control Procedures for Telex and Group 4 Facsimile Service Based on Recommendations X.215/X.225
T.70	Network Independent Basic Transport Service for the Telematic Services
T.80	Common Components for Image Compression and Communication: Basic Principles

Recommendation	Title
T.81	Digital Compression and Coding of Continuous-Tone Still Images
T.82	Digital Compression and Coding of Bi-Level Still Images
T.90	Characteristics and Protocols for Terminals for Telematic Services in ISDN
T.122	Multi-point Communications Service (MCUS)
T.123	Audio Visual Protocol Stack for Terminals and MCUS
T.124	Generic Conference Control Application for Audiovisual Conferencing and MCUS
T.400	Introduction of Document Architecture, Transfer and Manipulation
T.410	Open Document Architecture (ODA) and Interchange Format
T.411	Open Document Architecture (ODA) and Interchange Format: Introduction and General Principles
T.412	Open Document Architecture (ODA) and Interchange Format: Document Structures
T.414	Open Document Architecture (ODA) and Interchange Format: Document Profile
T.415	Open Document Architecture (ODA) and Interchange Format: Open Document Interchange Format (ODIF)
T.416	Open Document Architecture (ODA) and Interchange Format: Character Count Architectures
T.417	Open Document Architecture (ODA) and Interchange Format–Raster Graphics Content Architectures
T.431	Document Transfer and Manipulation (DTAM)–Services and Protocols–Introduction and General Principles
T.432	Document Transfer and Manipulation (DTAM)–Services and Protocols–Service Definition
T.433	Document Transfer and Manipulation (DTAM)–Services and Protocols–Protocol Specification
T.434	Binary File Transfer (BFT) Protocol for the Telematic Services
T.441	Document Transfer and Manipulation (DTAM) Services and Protocol: Document Transfer and Manipulation (DTAM) - Operational Structure
T.501	A Document Application Profile MM for the Interchange of Formatted Mixed Mode Documents
T.502	Document Application Profile PM1 for the Interchange of Processable Form Documents
T.503	A Document Application Profile for Interchange of Group 4 Facsimile Documents
T.505	Processable Mode
T.506	Document Application Profile PM-36 for the Interchange of Enhanced Mixed Content Documents in Processable and Formatted Forms
T.510	General Overview of the T.510 Series

Recommendation	Title
T.521	Communication Application Profile BTO for Document Bulk Transfer Based on the Session Service (according to rules defined in Recommendation T.62bis)
T.522	Communication Application Profile BT1 for Document Bulk Transfer
T.561	Terminal Characteristics for Mixed Mode of Operation MM
T.562	Terminal Characteristics for Telex Processable Mode of Operation PM.1
T.563	Terminal Characteristics for Group 4 Facsimile Apparatus
T.565	Terminal Characteristics for the Telematic Transfer Within the Facsimile Group 4 and Telex Service
T.611	Programmable Communication Interface (PCI) APLI/COM for Facsimile Group 3, Facsimile Group 4, Telex and Telex Service

ITU Data Communications Standard Recommendations

Recommendation	Title
X.1–X.32	Services and Facilities, Interfaces
X.40–X.181	Transmission, Signaling and Switching
X.200–X.219	Open Systems Interconnection (OSI) – Model and notation
X.220–X.290	Open Systems Interconnection (OSI) – Protocol Specifications
X.400–X.420	Message Handling Systems

ITU Operations and Quality of Service Standards Recommendations

Recommendation	Title
F.160–F.353	Telematic Services
F.600, F.601	Data transmission Services
F.710–F.703	Teleconferencing Services

EIA Fax Standards

Recommendation	Title
EIA-465	Group 3 Apparatus for Transmission (ITU T.4)
EIA-466	Procedures for Document Facsimile Transmission (ITU T.30)
EIA-578, EIA-592	Asynchronous Facsimile DCE Control

DOD Fax Standard

Recommendation	Title
MIL-STD-188-161C	Interoperability and Performance Standard for Digital Facsimile Equipment

Appendix B: Facsimile Machine Groups

What's in this Appendix

This appendix summarizes the standard groups mentioned in this document.

Standard Groupings

Fax machines are grouped into categories according to their capabilities. Chief among these capabilities are their transmission speed and image resolution (lines/page). The current standard is Group 3. Group 4 is a proposed future standard.

- **Group 1**
  Type: Analog
  Transmit speed: 300 baud
  Lines/min: 180
  Lines/page: 1080
  Min/page: 6
  Modulation: FM[1]
  White: 1300 Hz.
  Black: 2100 Hz.
  Image compression code: none
- **Group 2**
  Type: Analog
  Transmit speed: 1200 baud
  Lines/min: 360
  Lines/page: 1080
  Min/page: 3
  Modulation: VSB[2] AM[3]
  Carrier frequency: 2100 Hz.
  White: Maximum carrier
  Black: 26 dB below max.
  Image compression code: none
- **Group 3**
  Type: Digital over analog lines
  Transmit speed: ≥2400 baud
  Lines/min: 3,000 to 7,500 depending on the modem
  Lines/page: 1080, 2160 (fine)
  Min/page: 0.08 to 0.36 depending on the modem and resolution
  Modulation: 6 bit PAM[4]
  Black/White: Digitally encoded image
  Image compression code: Modified Huffman

[1] FM = Frequency Modulation
[2] VSB = Vestigial Sideband
[3] AM = Amplitude Modulation
[4] PAM = Pulse Amplitude Modulation

- **Group 4** (tentative)
  Type: Fully digital, cannot use analog lines
  Transmit speed: ≥19.2K baud, likely 56K baud or higher depending on the digital network used
  Lines/page: 2200, 3300, 4400,(fine)
  Min/page: <0.01, transmission, limited by the scanner
  Modulation: none, requires digital telephone network (ISDN)
  Black/White: Digitally encoded image
  Image compression code: Modified Huffman

Appendix C: Contacting CIAC

Phone	(510) 422-8193
Fax	(510) 423-8002
STU-III	(510) 423-2604
Electronic mail	ciac@llnl.gov
Emergency SKYPAGE	800-SKYPAGE pin# 855-0070
Anonymous FTP Server	ciac.llnl.gov (IP 128.115.19.53)
BBS	(510) 423-3331 (9600 Baud) (510) 423-4753 (2400 Baud)

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

_____

_____

_____

_____

_____

_____

_____

_____

List suggestions for improvement here.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Optional:

Name _____ Phone _____

Return address on back

Department of Energy

CIAC

Computer Incident Advisory Capability

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551